



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/899,837	07/09/2001	Mark R. Walker	P 279167 P11162	4039

27496 7590 11/23/2004

PILLSBURY WINTHROP LLP
725 S. FIGUEROA STREET
SUITE 2800
LOS ANGELES, CA 90017

EXAMINER

DINH, MINH

ART UNIT PAPER NUMBER

2132

DATE MAILED: 11/23/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/899,837

Applicant(s)

WALKER, MARK R.

Examiner

Minh Dinh

Art Unit

2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☐ Responsive to communication(s) filed on ____.
- 2a) ☐ This action is FINAL. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-26 is/are pending in the application.
- 4a) Of the above claim(s) 15-26 is/are withdrawn from consideration.
- 5) ☐ Claim(s) ____ is/are allowed.
- 6) ☒ Claim(s) 1-14 is/are rejected.
- 7) ☐ Claim(s) ____ is/are objected to.
- 8) ☐ Claim(s) ____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 09 July 2001 is/are: a) ☐ accepted or b) ☒ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. ____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date 10/09/2001.
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. ____.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: ____.

DETAILED ACTION

Election/Restrictions

1. Restriction to one of the following inventions is required under 35 U.S.C. 121:
 - I. Claims 1-14, drawn to an authentication method used in a network, classified in class 713, subclass 168.
 - II. Claims 15-26, drawn to a bridge connecting secure networks, classified in class 713, subclass 153.

The inventions are distinct, each from the other because of the following reasons:

Inventions I and II are related as subcombinations disclosed as usable together in a single combination. The subcombinations are distinct from each other if they are shown to be separately usable. In the instant case, invention I has separate utility such as authentication using encryption. See MPEP § 806.05(d).

2. Because these inventions are distinct for the reasons given above and have acquired a separate status in the art as shown by their different classification, restriction for examination purposes as indicated is proper.
3. Because these inventions are distinct for the reasons given above and have acquired a separate status in the art because of their recognized divergent subject matter, restriction for examination purposes as indicated is proper.

Art Unit: 2132

4. Because these inventions are distinct for the reasons given above and the search required for Group I is not required for Group II, restriction for examination purposes as indicated is proper.

5. During a telephone conversation with Mark Kendrick (RN 48468) on 11/09/04, a provisional election was made without traverse to prosecute the invention of group I, claims 1-14. Affirmation of this election must be made by applicant in replying to this Office action. Claims 15-26 are withdrawn from further consideration by the examiner, 37 CFR 1.142(b), as being drawn to a non-elected invention.

Drawings

6. The drawings are objected to as failing to comply with 37 CFR 1.84(p)(5) because they include the following reference character(s) not mentioned in the description: reference 'B' in figures 3(a)-3(b). Corrected drawing sheets in compliance with 37 CFR 1.121(d), or amendment to the specification to add the reference character(s) in the description in compliance with 37 CFR 1.121(b) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. The replacement sheet(s) should be labeled "Replacement Sheet" in the page header (as per 37 CFR 1.84(c)) so as not to obstruct any portion of the drawing figures. If the changes are not accepted by the

Art Unit: 2132

examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Claim Objections

7. Claims 1-2, 6-7 and 12 are objected to because of the following informalities: "otherwise encrypted key" (at the end of each claim) should be changed to "otherwise obfuscated key". Appropriate correction is required.

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

9. Claims 1-2, 6-7 and 11-12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Harney et al ("RFC 2093 – Group Key Management Protocol (GKMP) Specification") in view of Menezes et al ("Handbook of Applied Cryptography").

- a. Regarding claim 1, which is representative of claims 6 and 11, Harney discloses a method comprising:

in attempting to connect to one or more member peer nodes corresponding to one or more addresses on a connection list of addresses corresponding to member peer nodes of a semi-private peer network, sending a message encrypted using a

Art Unit: 2132

shared secret key from a connecting member peer node of the semi- private peer network to the one or more member peer nodes (Abstract; Section 1.1 Protocol Review, "The GKMP creates key ... the service is denied"; Section 2.1 Group Controller, "The GC helps ... that is the controller"; Section 6.1.3 Distributing Group Keys to Other Members, "send the key packet ... to the other members"); and

establishing a connection between the connecting member peer node and the one or more member peer nodes that successfully decrypt the encrypted message (Section 2.1 Group Controller, "The GC helps ... that is the controller").

The Harney method uses only a shared symmetric key for communications between peer nodes. Harney does not disclose using session keys. Menezes discloses generating a session key using a shared symmetric key by sending the session key encrypted using the shared symmetric key from a connecting node (p. 497-498, (i) Point-to-point key update using symmetric encryption, 1. key transport with one pass). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the Harney method to use session keys for communication sessions between peer nodes, as taught by Menezes. The motivation for doing so would have been to limit available ciphertext (under a fixed key) for cryptanalytic attack (p. 494, Motivation for use of session keys). Accordingly, the session key is encrypted and sent from the connecting node, and the connection is established only if the member peer node successfully decrypts the encrypted key.

b. Regarding claims 2, 7 and 12, Harney further discloses that the addresses are TCP/IP addresses (see Status of this Memo). Harney also discloses receiving an

Art Unit: 2132

acknowledgement from a peer node that successfully decrypts an encrypted key (Section 4.11 Key download ack).

10. Claims 3, 5, 8, 10 and 13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Harney in view of Menezes as applied to claims 1-2, 6-7 and 12 above, and further in view of Gong ("Enclaves: Enabling Secure Collaboration Over the Internet").

a. Regarding claims 3, 8 and 13, Harney does not disclose associating TCP port identifiers with the TCP/IP addresses. Gong discloses associating TCP port identifiers with the TCP/P addresses (p. 570, right column, 1st par., "Once a user initiates ... within the same group"). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combined method of Harney and Menezes to associate TCP port identifiers with the TCP/IP addresses, as taught by Gong. The motivation for doing so would have been that a user couldn't have more than one instance that is active within the same group.

b. Regarding claims 5 and 10, Harney does not disclose limiting establishing a connection to the one or more member peer nodes that are not connected to a same set of member peer nodes as an already connected member peer node. Gong discloses associating each member peer node with a particular port number and therefor, limiting establishing a connection to the one or more member peer nodes that are not connected to a same set of member peer nodes as an already connected member peer node. It would have been obvious to one of ordinary skill in the art at the

Art Unit: 2132

time the invention was made to modify the combined method of Harney and Menezes to associate each member peer node with a particular port number and therefor, to limit establishing a connection to the one or more member peer nodes that are not connected to a same set of member peer nodes as an already connected member peer node, as taught by Gong. Please refer to motivation recited for associating port identifiers with the TCP/IP addresses as taught by Gong in claim 3.

11. Claims 4, 9, and 14 rejected under 35 U.S.C. 103(a) as being unpatentable over Harney in view of Menezes as applied to claims 1, 6 and 11 above, and further in view of Waldman (WO 01/13201 A2). Harney does not disclose associating an encrypted key with the member peer node. Waldman discloses associating an encrypted password with each peer member; the password meets the limitation of a key (p. 5, lines 7-20). It would have been obvious to one of ordinary skill in the art at the time the invention was made to associate an encrypted key with the member peer node, as taught by Waldman. The motivation for doing so would have been that a peer node could perform authentication for other peer nodes (p. 4, lines 16-19).

Conclusion

12. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Traversat et al, US 2002/0147771 A1, Peer-To-Peer Computing Architecture.

Amir et al, "Exploring Robustness in Group Key Agreement".

Gong, "JXTA: A Network Programming Environment".

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Minh Dinh whose telephone number is 571-272-3802.

The examiner can normally be reached on Mon-Fri: 10:00am-6:30pm.


If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MD

Minh Dinh
Examiner
Art Unit 2132

MD
11/17/2004


GILBERTO BARRON
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100